Cybersecurity Culture in Civil Aviation

Published by authority of the Secretary General

January 2022

International Civil Aviation Organization

1. Introduction

This guidance is in line with the ICAO Aviation Cybersecurity Strategy[1], and the Cybersecurity Action Plan[2], which action item CyAP7.1 recommends to define and promote cybersecurity culture in civil aviation.

2. Scope

This guidance material aims to support Member States and stakeholders in designing and implementing a robust cybersecurity culture within their organizations. The ultimate objective is to support the security and resilience of civil aviation against cyber threats and risks.

3. Definition, general objectives, and benefits of cybersecurity culture

3.1 For the purposes of this guidance, cybersecurity culture is commonly understood to be a set of assumptions, attitudes, beliefs, behaviours, norms, perceptions, and values that are inherent in the daily operation of an organization and are reflected by the actions and behaviours of all entities and personnel in their interaction with digital assets.

3.2 A positive cybersecurity culture aims to make cybersecurity considerations part of the organization's habits, conducts, and processes, by embedding them in daily operations as reflected by the actions and behaviours of all personnel.

3.3 The establishment of a strong and effective cybersecurity culture, as an integral part of an organizational culture, assists organizations in improving their overall performance through the early identification of potential cyber risks.

3.4 Cybersecurity culture in civil aviation builds upon the sector's experience, efforts, and success in implementing robust aviation safety and security cultures, and shares with them many core elements. This cross-domain nature of cybersecurity culture not only leads to enhancing cybersecurity posture, but also results in positive spillovers across the three domains in supporting the promotion and reinforcement of positive safety, security and cybersecurity cultures.

3.5 In summary, cybersecurity culture allows every person in the organization, regardless of their role, to better perform in the digital environment. Examples of benefits of designing and implementing an effective and robust cybersecurity culture include:

a) enhanced cybersecurity maturity of the organization;
b) appropriate handling of information by all personnel;
c) improved cybersecurity posture that supports the effectiveness and efficiency of the organization in mitigating cyber risks;
d) enhanced awareness of all personnel to cyber risks and the role that they individually play in identifying and mitigating those risks; and
e) willingness to report personal oversight in applying organizational cybersecurity processes and procedures as well as reporting of suspicious cyber activities, leading to proactiveness and better detection of cyber risks.

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] ICAO State letter 2020/114

3.6 The core elements of an effective organizational aviation cybersecurity culture are illustrated in the following sections of this guidance. However, although these core elements are well defined, cybersecurity culture should be uniquely designed within each organization. It should take into account different aspects, including the organizational cybersecurity maturity level, existing cultures and values, and the overall cybersecurity threat landscape.

3.7 The core elements of a robust and effective cybersecurity culture in civil aviation are:

a) leadership;
b) cross-domain links;
c) communication;
d) awareness, training and education;
e) reporting systems;
f) continuous review and improvement; and
g) positive work environment.

4. **Leadership**

4.1 An effective cybersecurity culture depends on the commitment of every person in the organization, starting with senior management. Senior management should provide their full commitment to cybersecurity culture, at all times and across all activities, strategies, policies and organizational objectives.

4.2 Senior management should comply with cybersecurity policies, lead by example, and become role models for the organization's managers and personnel. They should also advocate for cybersecurity as an organizational and personal value while similarly working towards aligning their behaviours with such value.

4.3 In that regard, senior management should:

a) endeavour to enhance their knowledge of cybersecurity in civil aviation;
b) abide by cybersecurity rules, processes, and procedures at all times and lead by example;
c) clearly include cybersecurity as an organizational priority;
d) enshrine aviation cybersecurity in the written policies of the organization to become an integral part of the company's management plan;
e) provide visible support to the implementation of cybersecurity culture;
f) ensure and support cybersecurity training and capacity building for all personnel;
g) ensure the processing of cybersecurity reports in a timely fashion and ensure the prompt implementation of any required corrective and preventive actions;
h) intervene appropriately whenever cybersecurity is compromised; and
i) monitor the development of the cybersecurity posture of the organization, cybersecurity culture, and the measures and resources assigned to support the continuous improvement of cybersecurity culture's adoption across the organization.

4.4 Following the lead of senior management, the organization's management layers should also strive to adopt the actions included in paragraph 4.3, in line with their responsibilities and span of management, in order to propagate the commitment to cybersecurity culture across the organization.

5. **Cross-domain links**

5.1. Taking into account the multitude of cyber risks and vulnerabilities in every organization, cross-domain links should be formally established.

5.2. A multidisciplinary Task Force reporting to senior management might be established as a means to support coordination of cybersecurity culture across the organization.

5.3. The Task Force's objectives would include the following:

a) periodically assess the maturity of cybersecurity culture within the organization;
b) identify risks and opportunities with regards to cybersecurity culture implementation;
c) bridge the perspectives of different internal stakeholders with regards to cybersecurity culture; and
d) support the development and implementation of cross-domain activities related to fostering cybersecurity culture in the organization.

6. **Communication**

6.1. Communication plays an essential role, both internally and externally, in ensuring the implementation of successful cybersecurity culture. It is the main means through which the expected level of awareness can be reached.

6.2. In order for communication to be effective, certain skills should be considered as part of a robust cybersecurity culture:

a) *active listening* – process through which verbal and non-verbal signals are observed, in order to recognize the other individual's values and needs, and contribute to the improvement of team communication;
b) *adapting communication style to different audiences and situations* – understanding how others communicate and customizing the message in order to better reach them; and
c) *clarity of communication* – identify what and how to communicate.

6.3. Senior management should ensure that internal policies and guidelines regarding cybersecurity, as well as the reason for their introduction, are duly communicated to all personnel. A robust internal communication programme contributes to the acceptance and understanding of cybersecurity measures by all personnel, and helps promote cybersecurity culture in the organization.

6.4. In addition, internal communication programmes would greatly assist in:

a) ensuring that all personnel are fully aware of their duties, rights, and the reporting mechanisms in place in the organization; and
b) promoting the organizational digital code of conduct, that includes the processes, measures and controls that personnel should comply with at all times.

7. **Awareness, training and education**

7.1 Awareness, training and education are key areas of the learning process that should be leveraged for a robust cybersecurity culture. Awareness provides people with knowledge, training teaches skills, and education provides knowledge and skills within a theoretical framework, hence integrating awareness and training.

7.2 All civil aviation personnel who interact with the organization's digital assets, regardless of their roles or functions, should undertake a cybersecurity awareness, training, and education programme in order to ensure that they are equipped with required knowledge and skills on aviation cybersecurity risks, measures and objectives. These programmes should be adapted to the audience, as necessary and possible.

7.3 Cybersecurity awareness programmes should be delivered to all personnel upon their hiring, as well as a recurrent training. The time intervals for the recurrence of the awareness programme should be identified based on the level of maturity of cybersecurity culture in the organization, and can be revisited in line with the development of this maturity level.

7.4 It is recommended that cybersecurity awareness programmes be delivered at least once in person (in a physical or virtual classroom setting). Cybersecurity is not a familiar topic to all personnel and is sometimes hard to be digested without guidance from a professional. As such, interaction with a professional in a classroom setting facilitates the understanding of cybersecurity topics. It allows the trainer to explain concepts, processes, procedures, and controls in a simplified manner to be understood by the non-technically savvy personnel, as well as explain the benefits in enhancing the cybersecurity posture of the organization and its positive impact on the overall productivity of personnel.

7.5 Following an initial in-person awareness/training session, organizations may consider using e-learning methods (computer managed learning) for recurrent training. Such decision should take into account the development of cybersecurity culture in the organization, as well as changes in cybersecurity processes, controls, and procedures introduced in the organization in response to the evolving cybersecurity risk landscape.

7.6 Cybersecurity awareness programmes should be delivered by professionals that possess the required technical knowledge. However, one of the challenges faced with technical awareness programmes is the lack of soft skills by the presenters, whereby adequate communication and "sales" skills go a long way in engaging personnel and ensuring their buy-in and support to cybersecurity culture. Accordingly, organizations should ensure that awareness programme leaders are equally equipped with the technical knowledge and soft skills necessary to instil in personnel behavioural changes to support the adoption of cybersecurity culture.

7.7 A typical cybersecurity awareness programme should include the following subjects:

a) the purpose of the awareness programme;
b) existing communication mechanisms in the organization;
c) a general overview of cyber risks to civil aviation and potential consequences (including examples);
d) cybersecurity controls, processes, and procedures of the organization;
e) the role of the human element in safeguarding the organization against cyber risks;
f) the importance of personnel reminding each other of organizational cybersecurity principles when observing non-compliant actions by their colleagues;
g) overview of the different exploit methods that may target people and their consequences (including examples);
h) how to identify suspicious cyber activities;
i) the impact of complacency on the organization (including examples);
j) principles of cyber hygiene;
k) proper handling of sensitive data and information; and
l) reporting mechanisms, how to use them, and follow-up mechanisms.

7.8 Cybersecurity awareness campaigns should also be used periodically, as a reminder, in order to reinforce the knowledge and skills of personnel. Various tools are available for that purpose including:

a) *paper-based tools* – such as posters, brochures, booklets, etc. This type of media can be easily distributed and digested. However, they are passive tools and require frequent update (and a new print with each update); and

b) *online tools* – such as e-mails, newsletters, messages on screen savers, intranet, short videos, FAQ pages, e-learning (computer managed learning), etc. The main advantage of these tools compared to paper-based tools is their ability to reach the whole organization. They are relatively easy to update in terms of resources, and have a low production cost.

8. **Reporting systems**

8.1 A cornerstone of cybersecurity culture is the development and implementation of an internal cybersecurity reporting system. Such system allows the organization to proactively manage its cyber risks, measure the development of the organization's cybersecurity posture, identify and plan awareness and training needs of staff, and adapt its internal processes, controls, and measures in line with the development of cybersecurity trends and with the maturity of cybersecurity culture.

8.2 Cybersecurity reporting systems gather elements from both aviation safety and aviation security reporting systems. As such, they address two areas: the first area is reporting of self-actions/errors that are not in line with the organizational information security policies and processes, and the second area is reporting of suspicious/erroneous behaviour of other employees.

8.3 When developing their cybersecurity reporting mechanism, organizations are encouraged to benefit from the experience gained in developing and implementing aviation safety and aviation security reporting systems.

8.4 The following elements should be considered when implementing a cybersecurity reporting system:

a) confidentiality of personal information, whereby personal data is not collected and/or stored. When personal data is collected it should only be used to either gain clarification, further information about the reported occurrence or offer feedback to the reporter;
b) in order to ensure the confidentiality of personal information, a policy should be developed that clearly identifies, and holds accountable, the person(s) tasked with managing, maintaining, guaranteeing the confidentiality, analyzing, and following up on collected information;
c) providing adequate training to all personnel on how to use the reporting system;
d) implementing a just culture in cybersecurity reporting, and providing adequate awareness to all personnel on how a just culture works so that they are more comfortable providing information; and
e) implementing, as applicable, an incentive programme aimed at encouraging personnel to report their own errors as well as any suspicious cyber behaviours they observe.

Just culture

8.5 Organizations should encourage their personnel to report cybersecurity incidents through the adoption of a just culture. Just culture is a concept implemented in safety reporting which could be of great value in promoting a cybersecurity culture.

8.6 In a cybersecurity reporting context, a just culture encourages all personnel to report cybersecurity incidents and errors. It is an environment where everyone understands that they will be treated fairly based on their actions rather than the outcome of their actions. In a just culture environment, all personnel clearly understand that it is not fair to punish all errors regardless of their circumstances, while at the same time they also understand that it is unacceptable to provide a blanket immunity from punishment as some actions could have malicious intent, or could be the result of pure negligence and/or nonchalance. As such, it is important to draw the line between acceptable and unacceptable actions when designing a just culture.

8.7 A just culture not only defines the responsibilities of personnel towards their organizations, but also those of management towards personnel. Those responsibilities should be included in a policy in which the organization's senior management should:

a) encourage staff to practice cyber hygiene and commit to recognize their efforts in supporting the organization in managing cyber risks;
b) commit to provide all personnel with the adequate cybersecurity procedures, awareness, training, and education to support them in performing their duties;
c) assume responsibility if any incident is caused by lack of awareness or promptness in addressing a certain cyber risk; and
d) encourage staff to report cyber incidents, hazards, errors, or any suspicious behaviour they witness without fear of reprisal.

Quality control

8.8 Organizations should implement quality control programmes designed to monitor the effective implementation of cybersecurity measures. Quality control programmes can be an effective tool in keeping personnel alert and committed to cybersecurity culture principles. The frequency and rigidity with which quality controls are carried out may have a positive influence on personnel by demonstrating management's commitment to cybersecurity objectives and compliance.

8.9 Regular quality controls of the reporting mechanisms in place should be carried out as part of the quality control programmes.

9. Continuous review and improvement

9.1 Organizations should develop a performance indicator framework designed to assess the impact of measures in place on cybersecurity culture as well as to determine the gap existing between desired and actual culture outcomes.

9.2 As some elements of cybersecurity culture may not be directly observed, a range of possible indicators can be used to measure the effectiveness of cybersecurity culture. Such measures may include:

a) statistics on reported incidents (considered comparatively with data mined from the organization's logs) to measure cybersecurity performance of personnel, their level of awareness, and the progress achieved in promoting cybersecurity reporting;
b) results of recurrent training sessions;
c) results from simulations of malicious attacks to test response of personnel; and
d) questionnaires and interviews.

10. Positive work environment

10.1 A general positive work environment may also greatly influence commitment of personnel to cybersecurity culture and enhance cybersecurity performance.

10.2 A positive work environment should include, at a minimum:

a) the involvement of personnel in decision-making processes (e.g. suggestions for improvement to cybersecurity awareness training programmes);
b) the allocation of sufficient time for personnel to complete training on proper cyber hygiene;
c) a mechanism for recognizing good performance (i.e. incentives and/or reward programmes);
d) the provision of feedback to personnel on suggestions and on cybersecurity reports;

e) setting clear, achievable and measurable goals with regards to cybersecurity incidents, and periodic feedback to personnel on how the organization is advancing in that regard;
f) the provision of the necessary procedures, awareness, training, and tools to enable personnel to perform their duties; and
g) providing personnel with the appropriate levels of autonomy and responsibility.

— END —